Forenzika Digjitale

Trajtimi i të dhënave dhe atributi i sulmit

Forenzika Digjitale

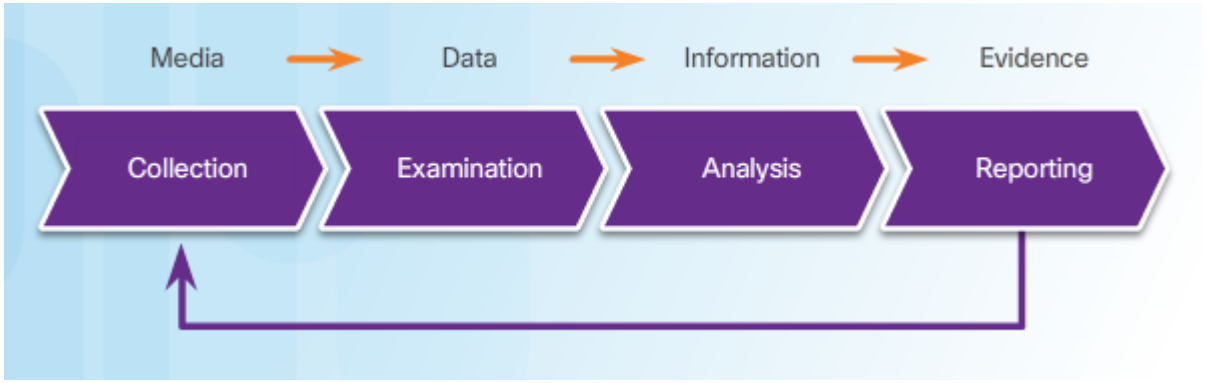
- Analisti i sigurisë kibernetike do të zbulojë prova të veprimtarisë kriminale.
  - Duhet të identifikojnë aktorët e kërcënimit, t'i raportojnë ato tek autoritetet përkatëse dhe të ofrojnë dëshmi për të mbështetur ndjekjen penale.
  - Zakonisht së pari duhet të zbulohet gabimi.
- Mjekësia ligjore dixhitale është rikuperimi dhe hetimi i informacionit të gjetur në pajisjet digjitale për sa i përket aktivitetit kriminal.
  - Mund të jenë të dhëna për pajisjet e ruajtjes, në kujtesën e paqëndrueshme të kompjuterit, ose gjurmët e krimit kompjuterik në të dhënat e rrjetit siç janë pcaps dhe shkrimet
- Aktiviteti kiberkriminal mund të karakterizohet si origjinë nga brenda ose jashtë organizatës.
- Sipas HIPAA, njoftimi i shkeljes duhet t'i bëhet individëve të prekur.
- Analistët duhet të dinë kërkesat në lidhje me ruajtjen dhe trajtimin e provave.

Trajtimi i të dhënave dhe atributi i sulmit

Procesi I Forenzikës Digjitale

- NIST përshkruan procesin e forenzikës dixhitale, duke përfshirë katër hapa:

1. Mbledhja - Identifikimi i burimeve të mundshme të të dhënave ligjore dhe përvetësimi, trajtimi dhe ruajtja e atyre të dhënave.
2. Ekzaminimi - Vlerësimi dhe nxjerrja e informacionit përkatës nga të dhënat e mbledhura. Mund të përfshijë decompression dhe decryption.
3. Analiza - Duke nxjerrë përfundime nga të dhënat. (Njerëzit, vendet, koha, ngjarjet, etj)
4. Raportimi - Përgatitja dhe paraqitja e informacionit. Duhen bërë sugjerime për hetime të mëtejshme dhe hapat e ardhshëm.



Llojet e provave

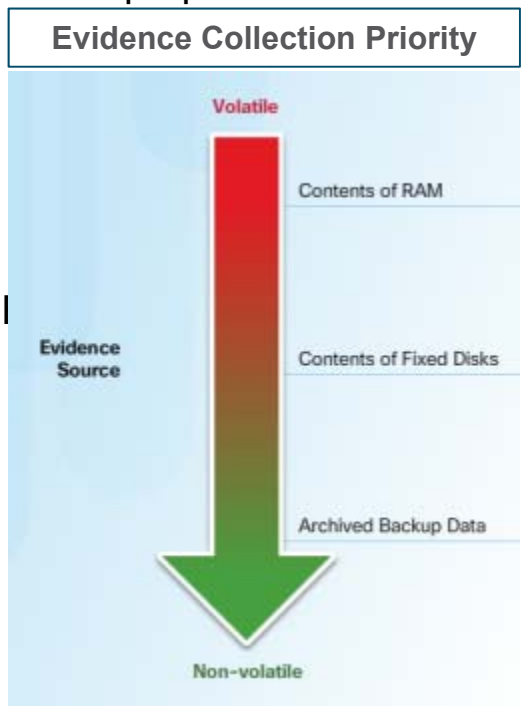
- Në procedurat ligjore, provat klasifikohen gjerësisht:
  - Dëshmitë e drejtpërdrejta ishin të padiskutueshme në posedim të të akuzuarit, ose dëshmia e dëshmitarit okular nga dikush që vëzhgonte sjelljen kriminale.
  - Prova më e mirë është dëshmi që është në gjendjen e saj fillestare.
  - Prova vërtetuese mbështet një pohim që është zhvilluar nga provat më të mira.
  - Dëshmia e tërthortë, në kombinim me fakte të tjera, krijon një hipotezë. Gjithashtu e di si dëshmi rrethanore.

Trajtimi i të dhënave dhe atributi i sulmit

Renditja e provave

- Mbledhja e dëshmive digjitale duhet të fillojë në mënyrë që nga provat më të paqëndrueshme dhe të vazhdojë deri në më pak të paqëndrueshme.
  - Të dhënat në RAM janë më të paqëndrueshme.
- Shembull më të paqëndrueshëm të paktën të paqëndrueshëm:

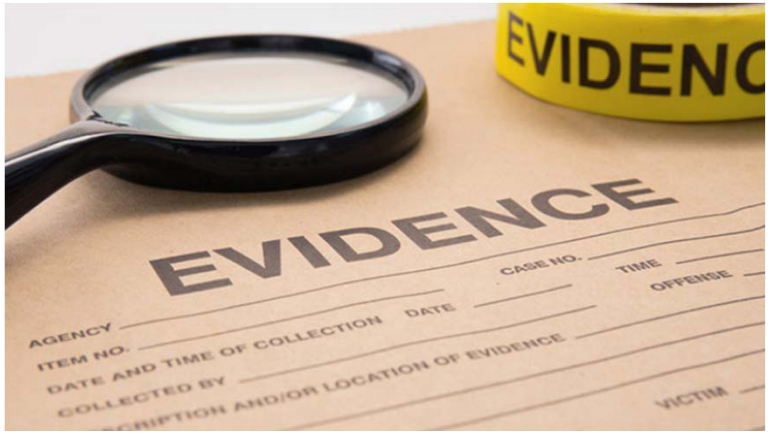
1. Regjistrat e kujtesës, arkëtimet
2. Tabela e drejtimit, cache ARP, tabela e procesit, statistikat e kernelit, l
3. Sisteme të përkohshme të skedarëve
4. Media jo të paqëndrueshme, të fiksuar dhe të lëvizshëm
5. Regjistrimi në distancë dhe të dhënat e monitorimit
6. Ndërlidhjet fizike dhe topologjitë
7. Media arkivore, shirit ose rezerva të tjera



Trajtimi i të dhënave dhe atributi i sulmit

Zinxhiri i Kujdestarisë

- Zinxhiri i kujdestarisë përfshin mbledhjen, trajtimin dhe ruajtjen e sigurt të provave.
  - Kush zbuloi provat.
  - Të gjitha detajet në lidhje me trajtimin e provave përfshirë kohën, vendet dhe personelin e përfshirë.
  - Kush ka përgjegjësinë kryesore për provat, kur është caktuar përgjegjësia dhe kur kujdesi ndryshon.
  - Kush ka qasje fizike në prova derisa është ruajtur? Qasja duhet të kufizohet vetëm në personelin më thelbësor.



Trajtimi i të dhënave dhe atributi i sulmit

Integriteti dhe Ruajtja e të Dhënave

- Dëshmia dixhitale duhet të ruhet në gjendjen e saj origjinale.
  - Dëshmitë origjinale duhet të kopjohen dhe analizat duhet të bëhen vetëm në kopje.
  - Timestampat mund të jenë pjesë e provave, kështu që hapja e dosjeve nga mediat origjinale duhet të shmanget.
- Procesi i përdorur për të krijuar kopje të provave duhet të regjistrohet.
- Mjetet e veçanta duhet të përdoren për të ruajtur provat mjeko-ligjore para se pajisja të mbyllet dhe prova të humbasë.
- Përdoruesit nuk duhet të shkëputin, shkëpusin ose fikën makinën e infektuar, përveç nëse nuk u është thënë nga personeli i sigurisë.

Trajtimi i të dhënave dhe atributi i sulmit

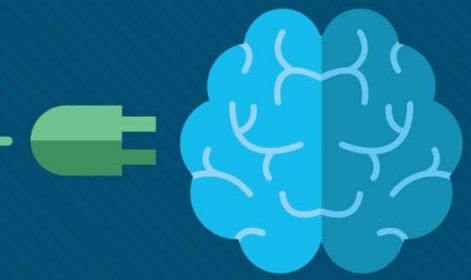
Atributi i sulmeve

- Atribuimi i kërcënimit është akti i përcaktimit të individit, organizatës ose kombit përgjegjës për një ndërhyrje të suksesshme ose incident të sulmit.
- Identifikimi i aktorëve të kërcënimit duhet të bëhet përmes hetimit parimor dhe sistematik të provave.
- Në një hetim të bazuar në prova, ekipi i reagimit të incidentit ndërlidhet me taktikat, teknikat dhe procedurat (TPP) që janë përdorur në incident me shfrytëzime të tjera të njohura për të identifikuar aktorët e kërcënimit.
- Aspektet e një kërcënimi që mund të ndihmojnë në atribuimin janë vendndodhja e hostëve ose domaineve me origjinë, tiparet e kodeve të përdorura në malware, mjetet e përdorura dhe teknika të tjera.

Përmbledhje

- Security Onion siguron një mjedis të integruar NSM për hetimin e ngjarjeve të sigurisë të krijuara nga sisteme të ndryshme.
- Një analist i nivelit 1 të sigurisë kibernetike vlerëson alarme të sigurisë për të verifikuar nëse incidentet aktuale të sigurisë kanë ndodhur.
- ELSA siguron një platformë të përbashkët të të dhënave për grumbullimin e dosjeve të logut nga shumë burime.
- Sguil siguron një konsol të analistit që mundëson hetimin e alarme nëpërmjet pivots në mjete të tjera.
- Analistët e Grupit 1 mund të zbulojnë aktivitetin e paligjshëm në rrjet dhe të kërkohet që të merren, ruajnë dhe analizojnë provat mjeko-ligjore digjitale.
- Dëshmitë digjitale mjeko-ligjore mund të çojnë në atributimin e ngjarjeve të sigurisë kibernetike tek aktorët kërcënues.

Përgjigjja dhe Trajtimi i Incidentit



CCNA Cybersecurity Operations v1.1

Objektivat

- Modelet e Reagimit të Incidentit
  - Aplikoni modelet e reagimit të incidentit në një ngjarje ndërhyrjeje.
    - Identifikoni hapat në Cyber Kill Chain.
    - Klasifikoni një ngjarje ndërhyrëse duke përdorur Modelin e Diamantit.
    - Aplikoni skemën VERIS në një incident.

- Trajtimi i Incidenteve
  - Zbatoni standardet e specifikuara në NIST 800-61r2 në një incident të sigurisë kompjuterike.
    - Përshkruani qëllimet e një CSIRT të dhënë
    - Zbatoni procedurat e trajtimit të incidentit NIST 800-61r2 në një skenar të caktuar incidenti.

The Cyber Kill Chain

Hapat e Cyber Kill Chain®

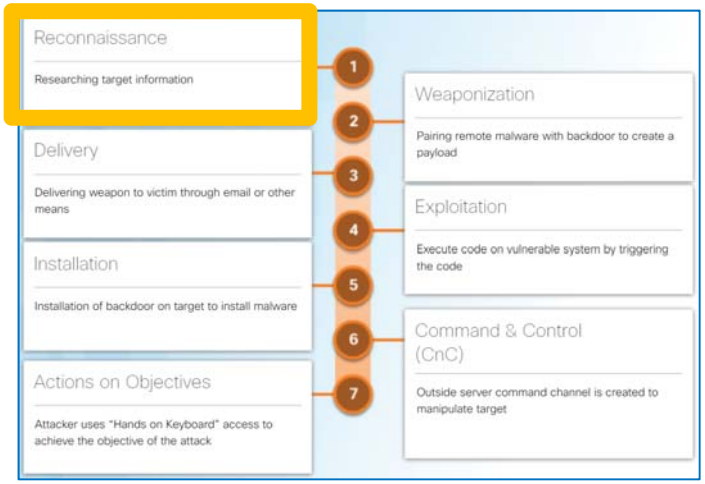
- Zhvilluar nga Lockheed Martin për të identifikuar dhe parandaluar ndërhyrjet kibernetike.
  - Hapat e Cyber Kill Zinxhiri ndihmojnë analistët të kuptojnë teknikat, mjetet dhe procedurat e aktorëve të kërcënimit.
  - Aktori i kërcënimit fiton më shumë akses ndaj objektivit ndërsa përparon përmes hapave.
  - Qëllimi është t'i ndaloni ato sa më shpejt që të jetë e mundur për të zvogëluar dëmet e bëra.

Steps of the Cyber Kill Chain

The Cyber Kill Chain

Zbulimi

- **Zbulimi** është kur aktori kërcënues kryen kërkime, mbledh inteligjencë dhe zgjedh objektiva.
- Organizatat mund të japin informacion mbi faqet e internetit, pajisjet e rrjetit që ballafaqohen me publikun, në artikujt e lajmeve, në procedurat e konferencave dhe në mediat sociale.

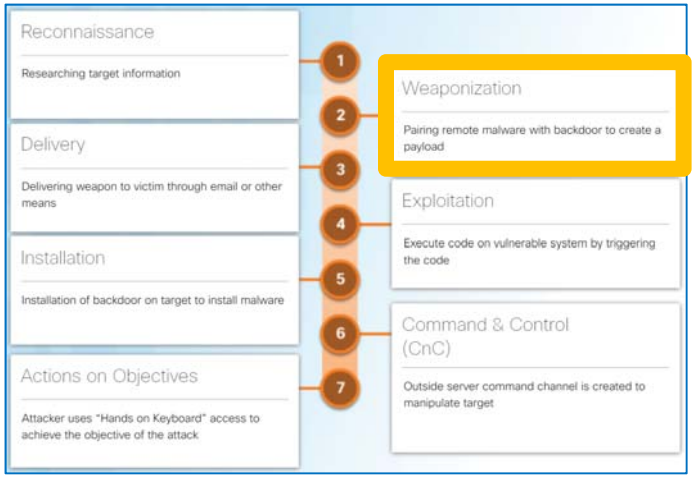


Adversary Tactics	SOC Defenses
Plan and conduct research: • Harvest email addresses • Identify employees on social media networks • Collect all public relations information (press releases, awards, conference attendees, etc.) • Discover Internet-facing servers	Discover Adversary's intent: • Web log alerts and historical searching data • Data mine browser analytics • Build playbooks for detecting browser behavior that indicate recon activity • Prioritize defense around technologies and people that recon activity is targeting

The Cyber Kill Chain

Weaponization

- **Weaponization** përdor informacionin e cenueshmërisë të mbledhur në hapin e zbulimit për të identifikuar dhe zhvilluar një armë kundër sistemeve specifike të synuara në organizatë.

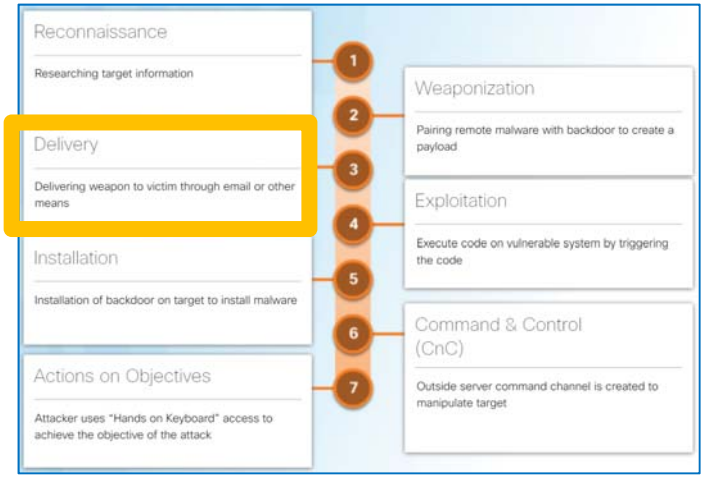


Adversary Tactics	SOC Defenses
Prepare and stage the operation: • Obtain an automated tool to deliver the malware payload (weaponizer). • Select or create a document to present to the victim. • Select backdoor and command and control infrastructure.	**Detect and collect weaponization artifacts:** • Conduct full malware analysis. • Build detections for the behavior of known weaponizers. • Is malware old, "off the shelf" or new malware that might indicate a tailored attack? • Collect files and metadata for future analysis. • Determine which weaponizer artifacts are common to which campaigns.

The Cyber Kill Chain

Delivery

- **Dorëzimi** është kur aktori kërcënues sjell armën e zhvilluar duke përdorur ose një faqe interneti, një media të lëvizshme USB ose një shtojcë të postës elektronike.



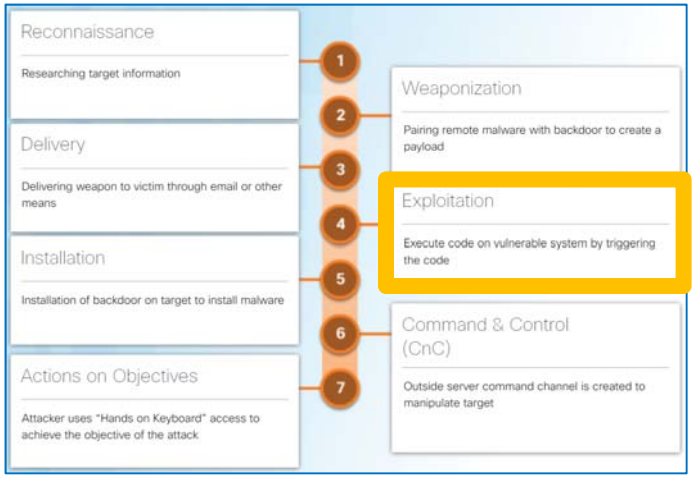
Adversary Tactics	SOC Defenses

Launch malware at target:
• Direct against web servers
• Indirect delivery through:
  • Malicious email
  • Malware on USB stick
  • Social media interactions
  • Compromised websites
	Block delivery of malware:
	• Analyze the infrastructure path used for delivery.
	• Understand targeted servers, people, and data available to attack.
	• Infer intent of the adversary based on targeting.
	• Collect email and web logs for forensic reconstruction.

The Cyber Kill Chain

Exploitation

- **Exploitation** është kur aktori kërcënues shkakton armë dhe e ekzekuton atë për të kompromentuar dobësinë dhe për të fituar kontrollin e objektivit.

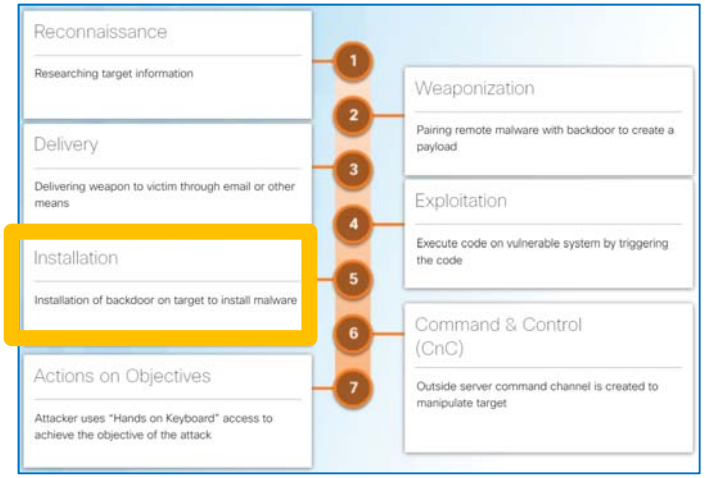


Adversary Tactics	SOC Defenses
Exploit a vulnerability to gain access: • Use a software, hardware, or human vulnerability • Acquire or develop the exploit • Use an adversary-triggered exploit for server vulnerabilities • Use a victim-triggered exploit such as opening an email attachment or a malicious web link	Train employees, secure code, and harden devices: • Employee awareness training and email testing • Web developer training for securing code • Regular vulnerability scanning and penetration testing • Endpoint hardening measures • Endpoint auditing to forensically determine origin of exploit

The Cyber Kill Chain

Installation

- **Installation** është kur aktori kërcënues krijon një derë e pasme në sistem për të lejuar hyrjen e vazhdueshme në objektiv.



Adversary Tactics	SOC Defenses
Install persistent backdoor: • Install webshell on web server for persistent access. • Create point of persistence by adding services, AutoRun keys, etc. • Some adversaries modify the timestamp of the malware to make it appear as part of the operating system.	**Detect, log, and analyze installation activity:** • HIPS to alert or block on common installation paths. • Determine if malware requires admin privileges or only user. • Endpoint auditing to discover abnormal file creations. • Determine if malware is known threat or a new variant.

The Cyber Kill Chain

Command and Control

- **Command & Control** (CnC or C2) është kur një kanal i jashtëm i serverit përdoret nga aktori kërcënues për të manipuluar një objektiv duke lëshuar komanda në softuerin që ata instaluan në objektiv.

Adversary Tactics	SOC Defenses
Open channel for target manipulation: • Open two way communications channel to CnC infrastructure. • Most common CnC channels are over web, DNS, and email protocols. • CnC infrastructure may be adversary owned or another victim network itself.	**Last chance to block operation:** • Research possible new CnC infrastructures. • Discover CnC infrastructure thorough malware analysis. • Prevent impact by blocking or disabling CnC channel. • Consolidate the number of Internet points of presence. • Customize blocks of CnC protocols on web proxies.

The Cyber Kill Chain

Veprimet mbi Objektivat

- **Veprimet mbi Objektivat** janë hapi i fundit i zinxhirit të vrasjeve dhe është kur sulmuesi arrin objektivin e sulmit.
  - Mund të përdoret për vjedhjet e të dhënave, kryerjen e një sulmi DDoS ose përdorimin e rrjetit të kompromentuar për të krijuar dhe dërguar spam.
  - Aktori i kërcënimit është thellësisht i rrënjosur në sistemet e organizatës dhe mund të jetë shumë e vështirë për t'u larguar nga rrjeti.

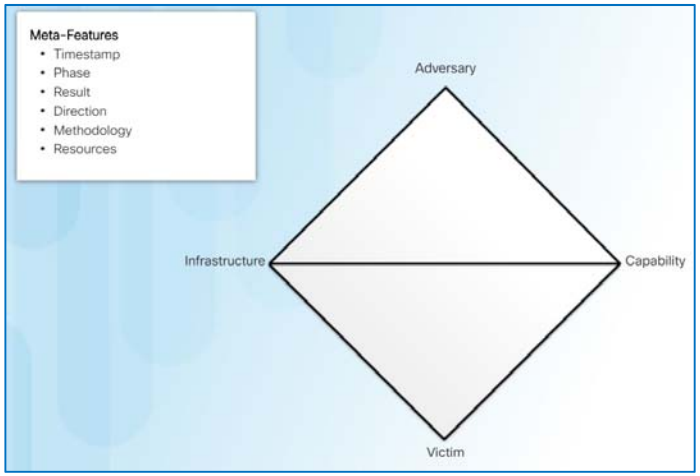
Adversary Tactics	SOC Defenses
Reap the rewards of successful attack: • Collect user credentials. • Privilege escalation. • Internal reconnaissance. • Lateral movement through environment. • Collect and exfiltrate data. • Destroy systems. • Overwrite, modify, or corrupt data.	Detect by using forensic evidence: • Establish incident response playbook. • Detect data exfiltration, lateral movement, and unauthorized credential usage. • Immediate analyst response for all alerts. • Forensic analysis of endpoints for rapid triage. • Network packet captures to recreate activity. • Conduct damage assessment.

Modeli i Diamantit të Ndërhyrjes

Përmbledhje e modelit të diamantit

- Modeli Diamond identifikon katër pjesë të përfshira në një incident të sigurisë.

Meta-features expand the model to include important elements.



- **Kundërshtari -** Palët përgjegjëse për ndërhyrjen.
- **Aftësi -** Vegël ose teknikë e përdorur nga aktori kërcënues.
- **Infrastruktura -** Rruga (rrjetet) e rrjetit të përdorur nga aktori kërcënues për të krijuar dhe mbajtur komandën dhe kontrollin.
- **Viktima -** Synimi i sulmit. Viktima mund të përdoret si pjesë e infrastrukturës për të nisur sulme të tjera**.**

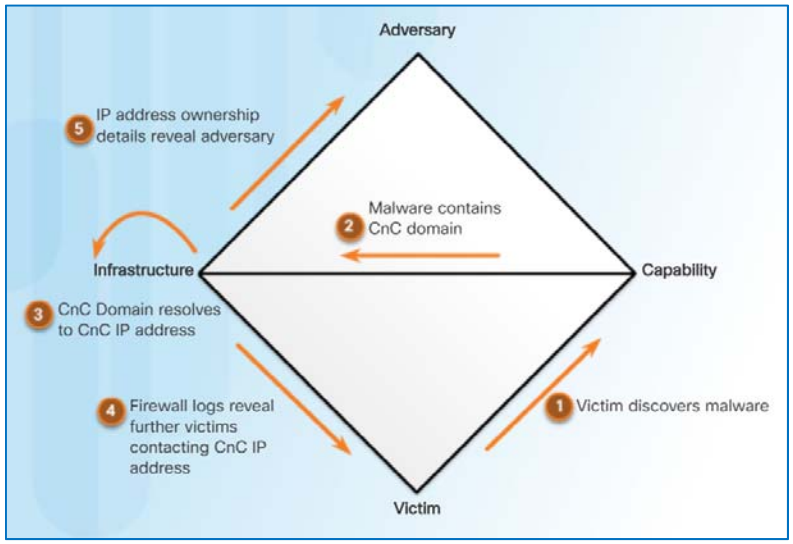
- Kundërshtari përdor aftësi mbi infrastrukturën për të sulmuar viktimën.
  - Çdo rresht në model tregon se si secila pjesë ka arritur në tjetrën.

Modeli i Diamantit të Ndërhyrjes

Pivoting Nëpër Modeli Diamond

- Modeli i Diamantit është ideal për të ilustruar se si kundërshtari kalon nga një ngjarje në tjetrën.

For example

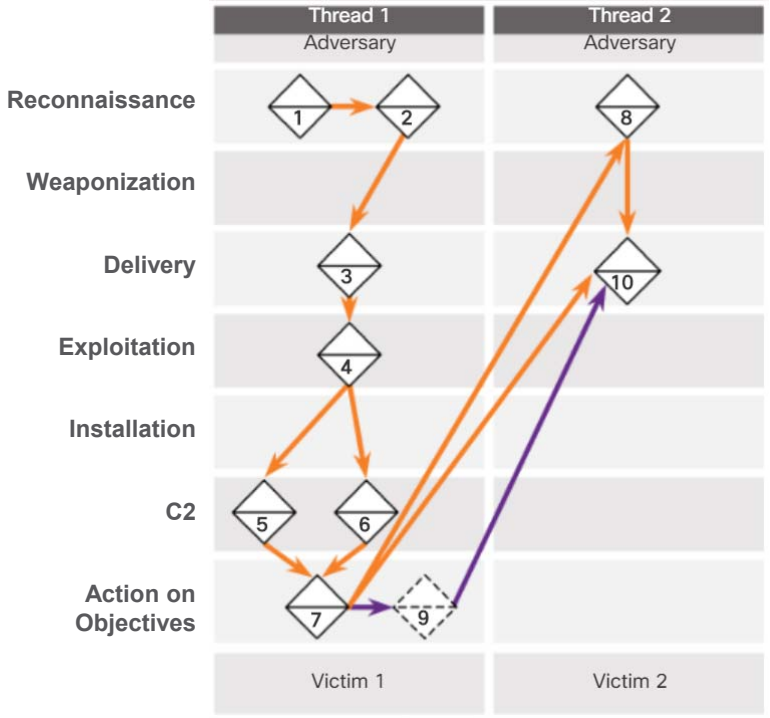


1) Një punonjës raporton se kompjuteri i tij po vepron jo normalisht dhe një skanim tregon se kompjuteri është i infektuar me malware.
2) Një analizë e malware zbulon se malware përmban një listë të emrave të domain CnC.
3) Këto emra domain zgjidhen në një listë të adresave IP.
4) Këto adresa IP përdoren për të hetuar shkrimet për të përcaktuar nëse viktimat e tjera në organizatë po përdorin kanalin CNN.
5) Adresat IP përdoren gjithashtu për të identifikuar kundërshtarin.

Modeli i Diamantit të Ndërhyrjes

Modeli i Diamantit dhe Cyber Kill Chain

- Shembulli ilustron procesin e përdorur nga një kundërshtar gjatë kalimit të Cyber Kill Chain.



1) Adversary bën një kërkim në internet për kompaninë e viktimave Gadgets, Inc. duke marrë si pjesë të rezultateve gadgets.com e tyre të domain.

2) Kundërshtari kërkon "administratorin e rrjetit gadget.com" dhe zbulon adresat e emailit të administratorëve të rrjetit.

3) Adversary dërgon email phishing me një kalë trojan bashkangjitur administratorëve të rrjetit.

4) Një administrator i rrjetit (NA1) hap lidhjen me qëllim të keq që ekzekuton shfrytëzimin e mbyllur.

5) Regjisori i NA1 regjistron me një kontrollues CNC duke dërguar një mesazh Postë HTTP dhe duke marrë një përgjigje HTTP në kthim.

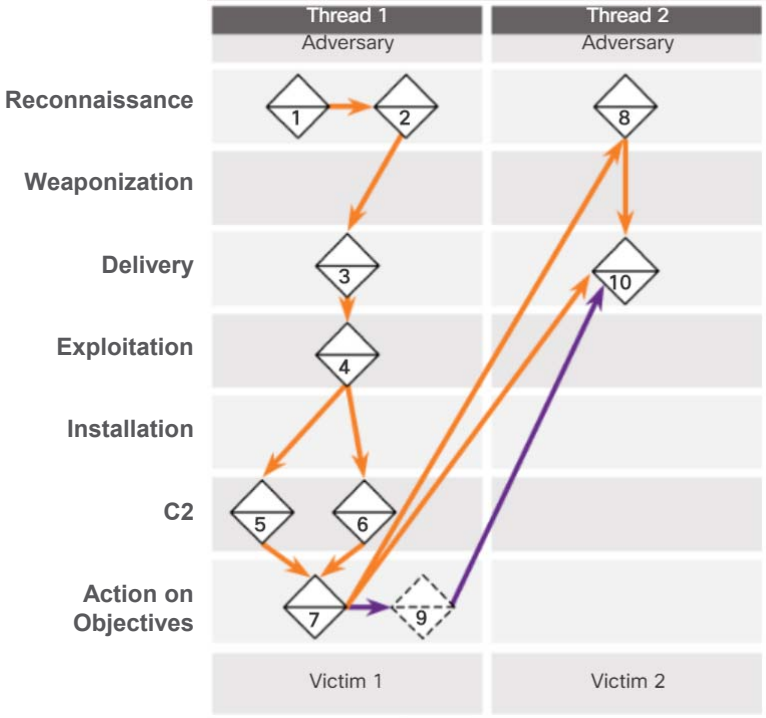
6) Analiza e malware identifikon adresa të tjera rezervë IP.

7) Përmes një mesazhi të përgjigjes HTTP të CnC dërguar tek nikoqiri i NA1, malware fillon të veprojë si një proxy për lidhjet e reja TCP.

Modeli i Diamantit të Ndërhyrjes

The Diamond Model and the Cyber Kill Chain (vazh.)

- Shembulli ilustron procesin e përdorur nga një kundërshtar gjatë kalimit të Cyber Kill Chain.



8) Nëpërmjet prokurorit të vendosur në hostin e NA1, kundërshtari bën një kërkim në internet për "hulumtimin më të rëndësishëm ndonjëherë" dhe gjen viktimën 2, Interesting Research Inc.

9) Kontrabandist kontrollon listën e kontakteve me email të NA1 për çdo kontakt nga Interesting Research Inc. dhe zbulon kontaktin për Zyrtarin Kryesor të Kërkimeve të Interesant Research Inc.

10) Zyrtari kryesor i Kërkimeve të Interesimit Research Inc. merr një email nga shtypi nga adresa e emailit e NA1 e Gadget Inc. dërguar nga pritësja e NA1 me të njëjtën ngarkesë që është vërejtur në Eventin 3.

Kundërshtari tani ka dy viktima të kompromet uara nga të cilat mund të nisin sulme të tjera.

Skema VERIS

Cila është Skema VERIS?

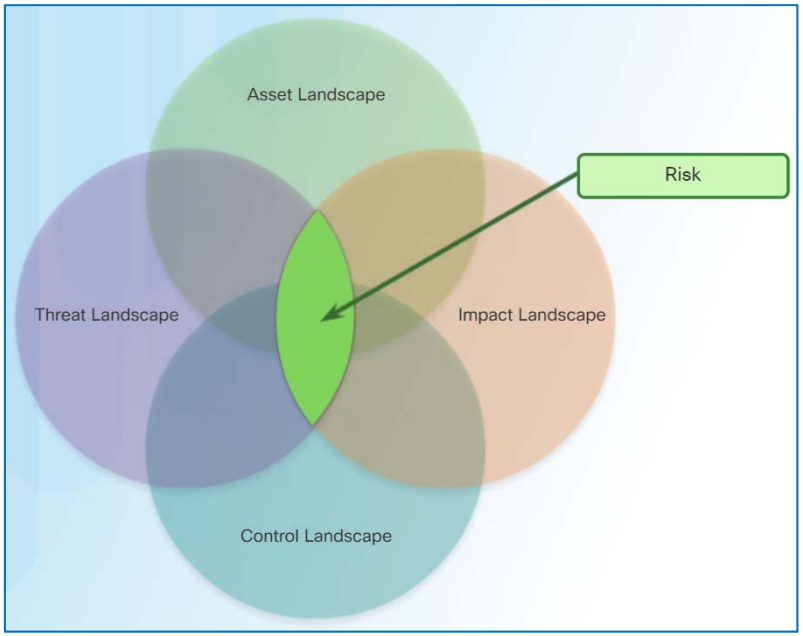
- Vocabulari për regjistrimin e ngjarjeve dhe për shpërndarjen e incidenteve (VERIS) është një grup metrikë për të përshkruar incidentet e sigurisë në një mënyrë të strukturuar.

- Në skemën VERIS, rreziku është përcaktuar si kryqëzim i katër peizazheve të Kërcënimit, Pasurisë, Ndikimi dhe Kontrollit.

- Informacioni nga çdo peizazh ndihmon për të kuptuar nivelin e rrezikut për organizatën.

- VERIS ndihmon në përcaktimin e këtyre peizazheve duke përdorur incidente reale të sigurisë për të ndihmuar në vlerësimin e menaxhimit të rrezikut.

VERIS schema



Skema VERIS

Krijimi I një VERIS Record

- Kur krijoni të dhëna për të shtuar në bazën e të dhënave, filloni me faktet themelore rreth incidentit dhe përdorni elementët VERIS të përvijuara nga komuniteti.
  - Fushat e vetme të kërkuara në procesverbalin janë ato ku atributi është i pranishëm.
  - Sa më shumë dihet për incidentin, të dhënat mund të shtohen.

Variable	Value
timeline.incident.year	2017
schema_version	1.3
incident_id	1
security_incident	Confirmed
discovery_method	Unknown
action	Unknown
asset	Unknown
actor	Unknown
attribute	Unknown

- Informacion shtesë mund të regjistrohet duke shtuar etiketat VERIS në regjistrin ekzistues.

timeline.incident.year	2017
timeline.incident.month	06
timeline.incident.day	20

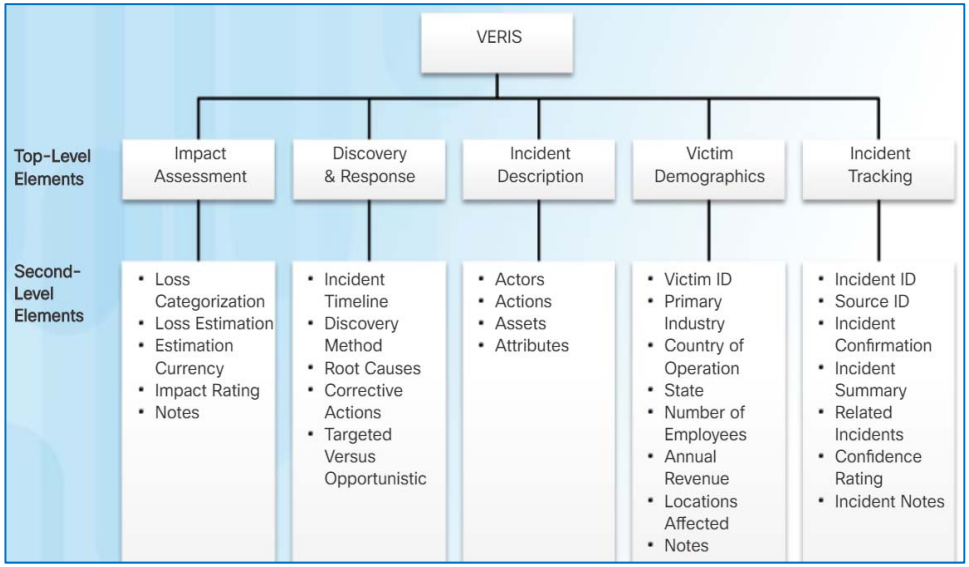
summary	Computer was infected with malware

discovery.notes	Reported by Debbie in sales
malware.notes	rootkit was found on Debbie's computer
social.notes	Debbie brought in an infected USB drive and used it on her company laptop

Skema VERIS

Elemente të nivelit të lartë dhe të nivelit të dytë

- Skema VERIS identifikon pesë elemente të nivelit të lartë, duke siguruar një aspekt tjetër të incidentit.
  - Secili element i nivelit të lartë përmban disa elemente të nivelit të dytë për klasifikimin e të dhënave të



- **Vlerësimi i Ndikimit -** Të gjitha incidentet kanë ndikim, qofshin ato të vogla apo të përhapura, të cilat mund të përcaktohen vetëm pas një incidenti të ndodhur.
- **Zbulimi dhe Përgjigja -** Identifikon afatet kohore të ngjarjeve, metodën e zbulimit të incidentit dhe çfarë përgjigjeje ishte për incidentin, duke përfshirë atë se si u riparua.
- **Përshkrimi i incidentit -** Përshkruan plotësisht një incident, duke përdorur modelin e kërcënimit A4 të zhvilluar nga Verizon.
- **Demografia e viktimave -** Përshkruan organizatën që ka përjetuar incidentin dhe karakteristikat e tij.
- **Ndjekja e incidentit -** Regjron informacione të përgjithshme rreth incidentit në mënyrë që organizatat të identifikojnë, ruajnë dhe rifitojnë incidentet me kalimin e kohës.

Skema VERIS

Baza e të dhënave të komunitetit VERIS

- Baza e të dhënave të komunitetit VERIS (VCDB) është një bazë të dhënash shumë e dobishme për organizatat që dëshirojnë të marrin pjesë.
  - Organizatat mund të dorëzojnë detajet e incidenteve të sigurisë në VCDB për komunitetin që të përdorë.
  - Sa më i madh dhe më i fuqishëm që VCDB të bëhet, aq më e dobishme do të jetë parandalimi, zbulimi dhe riparimi i incidenteve të sigurisë.
  - Ai gjithashtu do të bëhet një mjet shumë i dobishëm për menaxhimin e rrezikut, ruajtjen e të dhënave të organizatave, kohën, përpjekjet dhe paratë.